

## **REMARKS**

Claims 1, 3-16 and 18-20 (of which claims 1, 19 and 20 are independent) are currently pending. In the Office Action mailed May 6, 2004, claims 1 and 3-8 were rejected under 35 U.S.C. § 102(e), claims 1, 3-9, 11-13, 15-16 and 18-20 were rejected under 35 U.S.C. § 102(b), and claims 10 and 14 were rejected under 35 U.S.C. § 103(a).

### **I. Claims Rejections under 35 U.S.C. § 102(e)**

Claims 1 and 3-8 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Walker et al., U.S. Patent Number 6,061,723 (Walker). To anticipate a claim, each and every element set forth in the claim must be found in a single reference. (MPEP § 2131). Applicants submit that Walker does not teach “considering the location of the network device causing each event in the plurality of events by, for each event, determining the number of devices and/or links between the device causing the event and the network management station,” and “determining as said causal event, the event for which the determined number of devices and/or links is the fewest,” as in claim 1.

Walker teaches a network management system (“netmon”) that discovers the topology of a network using a criticalRoute attribute. After discovering devices on the network, the attribute then polls the network interfaces to determine whether each interface is up, down or if its status is unknown. (Walker, Col. 6, lines 22-27). Walker teaches that after checking the status of interfaces along the route for the interface in question (IIQ), netmon verifies whether failed interfaces are still down. While verifying, Walker teaches that netmon continues to poll other interfaces in the network. (Walker, Col. 8, lines 59-61). Some of these remaining interfaces may be inaccessible due to failed interfaces, and thus, Walker teaches that it “would be very

inefficient to verify the status of the entire criticalRoute for each secondaryFailure interface.”  
(Walker, Col. 8, lines 65-67).

To determine which of “interface down” events are primary failures, and which other “interface down” events are due to a secondary failure (i.e. resulting from the primary failure), Walker teaches an algorithm to examine the status of every interface along the criticalRoute to the interface that is down. (Walker, Col. 7, line 22 to Col. 8, line 48).

Consequently, Walker does not teach “considering the location of the network device causing each event” as in claim 1. The location of the interface in question is not considered by the algorithm taught in Walker. Instead the status of each interface along the critical route is determined by analyzing the stored status and, if necessary, polling each device to determine its status. Thus, Walker does not teach “considering the location of the network device causing each event” during any steps of the disclosed algorithm. In fact, Walker explicitly teaches to “avoid wasting time sending additional pings” to determine locations of all interfaces in question and if they are causing primary failures. (Walker, Col. 9, lines 5-9).

Further, although Walker teaches a number of configurations and filters used to classify interface failures, none of the methods taught in Walker include “determining as said causal event, the event for which the determined number of devices and/or links is the fewest,” as in claim 1. For example, Walker teaches that users can define network nodes to be members of a class, such as critical and regular, and interfaces are then analyzed accordingly. (Walker, Col. 12, lines 20-32). However, Walker does not teach counting the number of devices and/or links between the device causing the event and the network management station, as in claim 1.

The Examiner contends that within Walker, “the manager would look at the topology status map to determine that the closest link to the manager is the causal event.” (Office Action,

5.06.04, p. 3). The Examiner further contends that since the system in Walker is used with the OpenView Network Node Manager product, then managers may view the network configuration, and the managers would inherently select the closest link to the manager as the causal event. (Office Action, 5.06.04, p.3). However, Walker does not include any support for these contentions. Applicants submit that to anticipate a claim, each and every element set forth in the claim must be found in a single reference. (MPEP § 2131). Since Walker does not include any teaching of “determining as said causal event, the event for which the determined number of devices and/or links is the fewest,” then Walker cannot anticipate pending claim 1.

Furthermore, the Examiner contends that claim 1 “does not include any language that requires an algorithm or other automatic process to perform the critical steps of performing a count and then determining the causal event based on the count.” (Office Action, 5.06.04, p. 11). Applicants have amended claim 1 to recite that “the method [is] performed by said network management station.” Thus, claim 1 now includes language that requires an automatic process, and is allowable for at least this reason.

Thus, since Walker does not teach all the claim limitations of claim 1, then Walker fails to anticipate claims 1 and 3-8.

## **II. Claims Rejections under 35 U.S.C. § 102(e)**

Claims 1, 3-9, 11-13, 15-16 and 18-20 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Harris, U.S. Patent Number 5,771,274 (Harris). Like Walker, Applicants submit that Harris does not teach “considering the location of the network device causing each event in the plurality of events by, for each event, determining the number of devices and/or links between the device causing the event and the network management station,” and “determining as

said causal event, the event for which the determined number of devices and/or links is the fewest,” as in claims 1 and 19-20.

Harris teaches a telecommunications network in which Remote Monitoring Systems (RMSs) are employed. (Harris, Col. 3, lines 37-49). RMSs collect data from network devices including fault alarm messages and send the collected data to a central Fault Management System (FMS). (Harris, Col. 3, lines 49-51). The FMS generates fault alarm messages that are presented to a user on a user fault alarm display and control command interface.

Harris further teaches that a search is conducted to locate a connection point causing an alarm upon receiving alarm messages. The search results include a segment sequence number, which indicates the relative location of the equipment point along a circuit route that is causing a failure. (Harris, Col. 5, lines 32-59). By way of example, and as described at column 4, line 25 to column 5, line 31, Figure 3 in Harris illustrates one circuit 301 comprising three segments 302, 303 and 304 that would be identified in the topology data segment table (column 5, lines 19 to 31) with the same “circuit identifier” but separate “segment numbers” (e.g. 1, 2 and 3, respectively). Circuit 301 includes network devices (equipment) and links (carrier trunks), but note that the segment number relates to a segment comprising a pair of DS-3 ports and in most cases a fiber-optic trunk. However, the circuit is part of the network monitored by an RMS and *is not connected to the FMS*. Thus, contrary to the Examiner’s assertions, the use of segment sequence numbers does not equate to “determining the number of devices and/or links between the device causing the event *and the network management station*,” as in claim 1. (Emphasis added).

Moreover, because Harris teaches using segment sequence numbers to describe a relative location of equipment along a circuit route, Harris does not teach or suggest performing any

count of devices, as in claim 1. Instead, Harris uses the segment sequence numbers to correlate events. For example, at column 5, lines 51 to 55, Harris states that “if any alarm conditions are associated to the same circuit identifier, then it is possible to relate the given alarm to the others, topologically, using the sequence numbers.”

The Examiner further alleges that Harris discloses “determining as said causal event, the event for which the determined number of devices and/or links is the fewest” on the basis that the sequence numbers and relative locations are used to determine which events are from “upstream” devices and which are “significant alarm events.” (Office Action, 5.06.04, p. 6). However, as explained above, Harris does not count the number of devices and/or links, and thus, there is no mention that a lowest count constitutes a significant event.

In contrast, in relation to evaluating the significance of a given alarm in a plurality of related alarms, Harris teaches to determine whether another alarm is “upstream” from and in the same traffic direction as the given alarm point or another alarm is “upstream” and in the opposite direction, by using a “device type”, “alarm type” and, most importantly, a complex set of rules in the form of “truth tables” or a “rule based inference engine.” (Harris, Col. 6, lines 1 to 9). No count of the number of devices is used, as in claim 1.

Thus, since Harris does not teach all the claim limitations of claims 1 and 19-20, then Harris fails to anticipate claims 1, 3-9, 11-13, 15-16 and 18-20.

### **III. Claims Rejections under 35 U.S.C. § 103(a)**

Claims 10 and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Harris. Claims 10 and 14 depend from claim 1, which is not anticipated by Harris as explained above.

**IV. Summary**

Applicants respectively submit that in view of the remarks above, all of the pending claims 1, 3-16 and 18-20 are in condition for allowance and such action is respectively requested. The Examiner is invited to call the undersigned at (312) 913-0001 with any questions or comments.

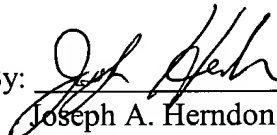
Respectfully submitted,

**McDonnell Boehnen Hulbert & Berghoff LLP**

Date: \_\_\_\_\_

9/3/04

By: \_\_\_\_\_

  
Joseph A. Herndon  
Reg. No. 50,469